Dynamic VLANs in tunnel mode

1. Introduction & operation

In most WLAN systems, each WLAN has a static policy that applies to all clients associated with a Service Set Identifier (SSID), or WLAN in the controller terminology. Although powerful, this method has limitations because it requires clients to associate with different SSIDs in order to inherit different QoS and security policies.
However, the Fortinet WLAN solution supports identity networking. This allows the network to advertise a single SSID, but allows specific users to inherit different QoS or security policies based on the user credential.

Dynamic VLAN assignment is one such feature that places a wireless user into a specific VLAN based on the credentials supplied by the user. This task of assigning users to a specific VLAN is handled by a RADIUS authentication server, such as FreeRadius or NPS server. This can be used, for example, to allow the wireless host to remain on the same VLAN as it moves within a campus network.
Therefore, when a client attempts to associate to a FortiAP registered with a controller, the FortiAP passes the credentials of the user to the RADIUS server for validation. Once the authentication is successful, the RADIUS server passes certain Internet Engineering Task Force (IETF) attributes to the user. These RADIUS attributes decide the VLAN ID that should be assigned to the wireless client. The SSID of the client does not matter because the user is always assigned to this predetermined VLAN ID.

The RADIUS user attributes used for the VLAN ID assignment are:

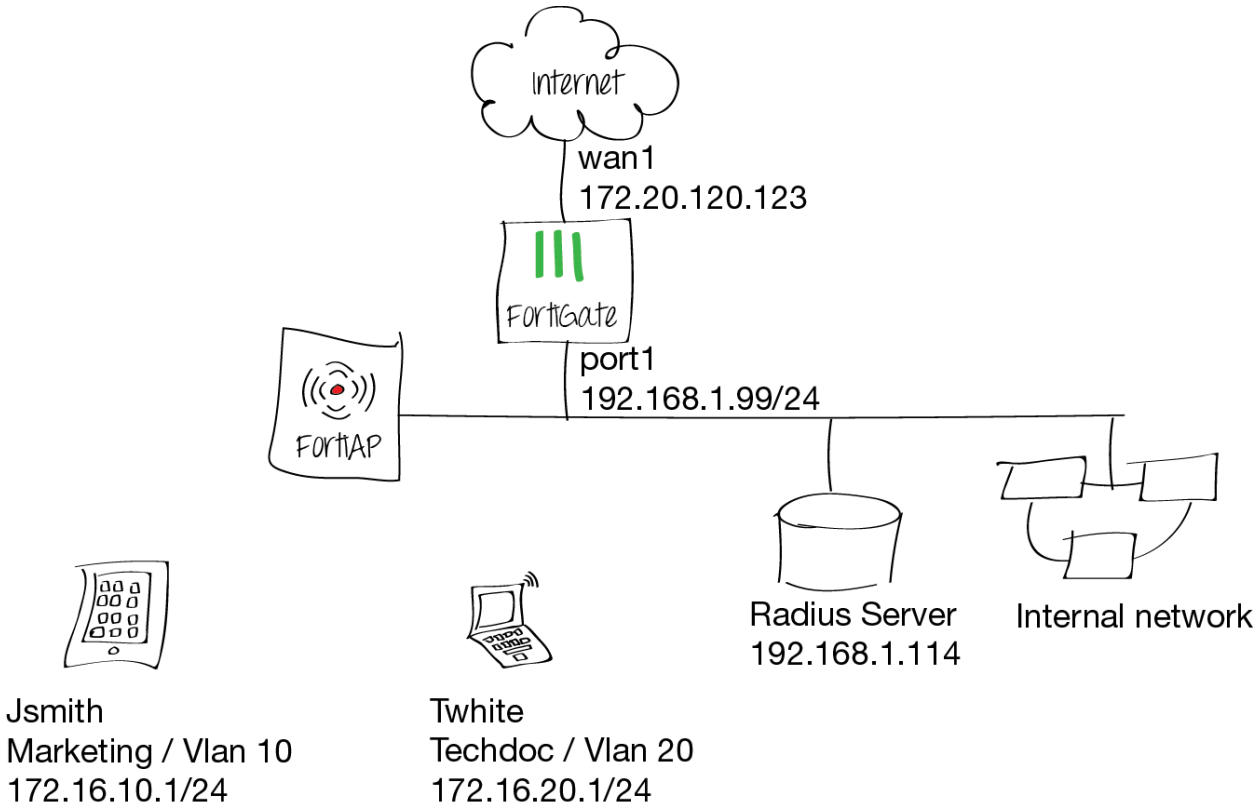
IETF 64 (Tunnel Type)—Set this to VLAN.
IETF 65 (Tunnel Medium Type)—Set this to 802
IETF 81 (Tunnel Private Group ID)—Set this to VLAN ID.

If dynamic-vlan is not enabled, all clients' traffic will use SSID's default vlan id.

If dynamic-vlan is enabled and a vlan id is configured on the radius server, the client will use the vlan id stored on the radius server; if not, it will use the SSID's default vlan id.

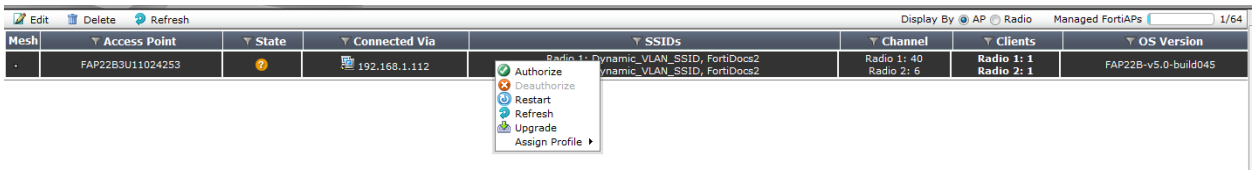
This feature is mainly implemented on the FortiAP. A combo command "cw_diag show wllbr" is provided to dump vlan info on the FortiAP.

2. Network topology

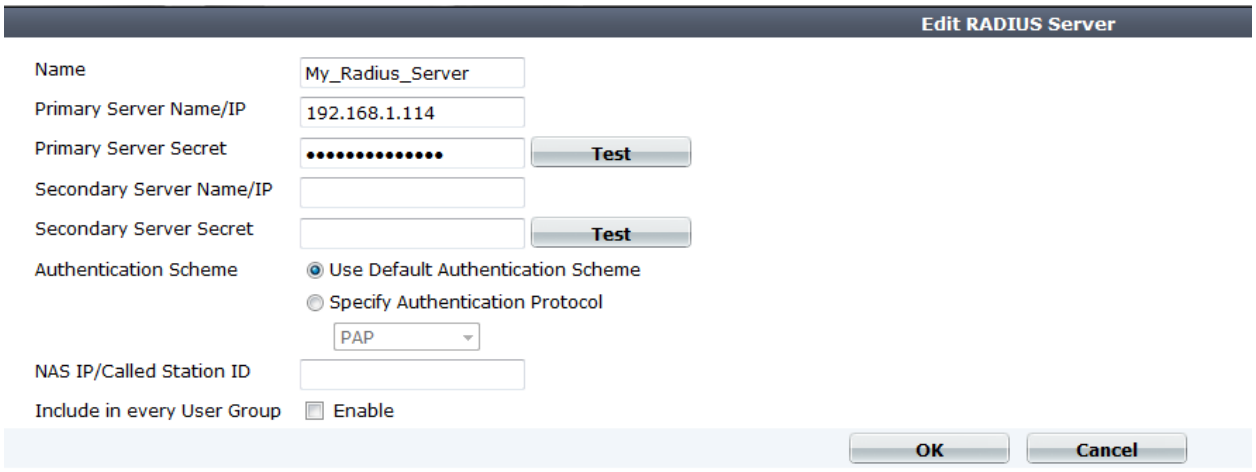


3. Configuring FortiGate unit

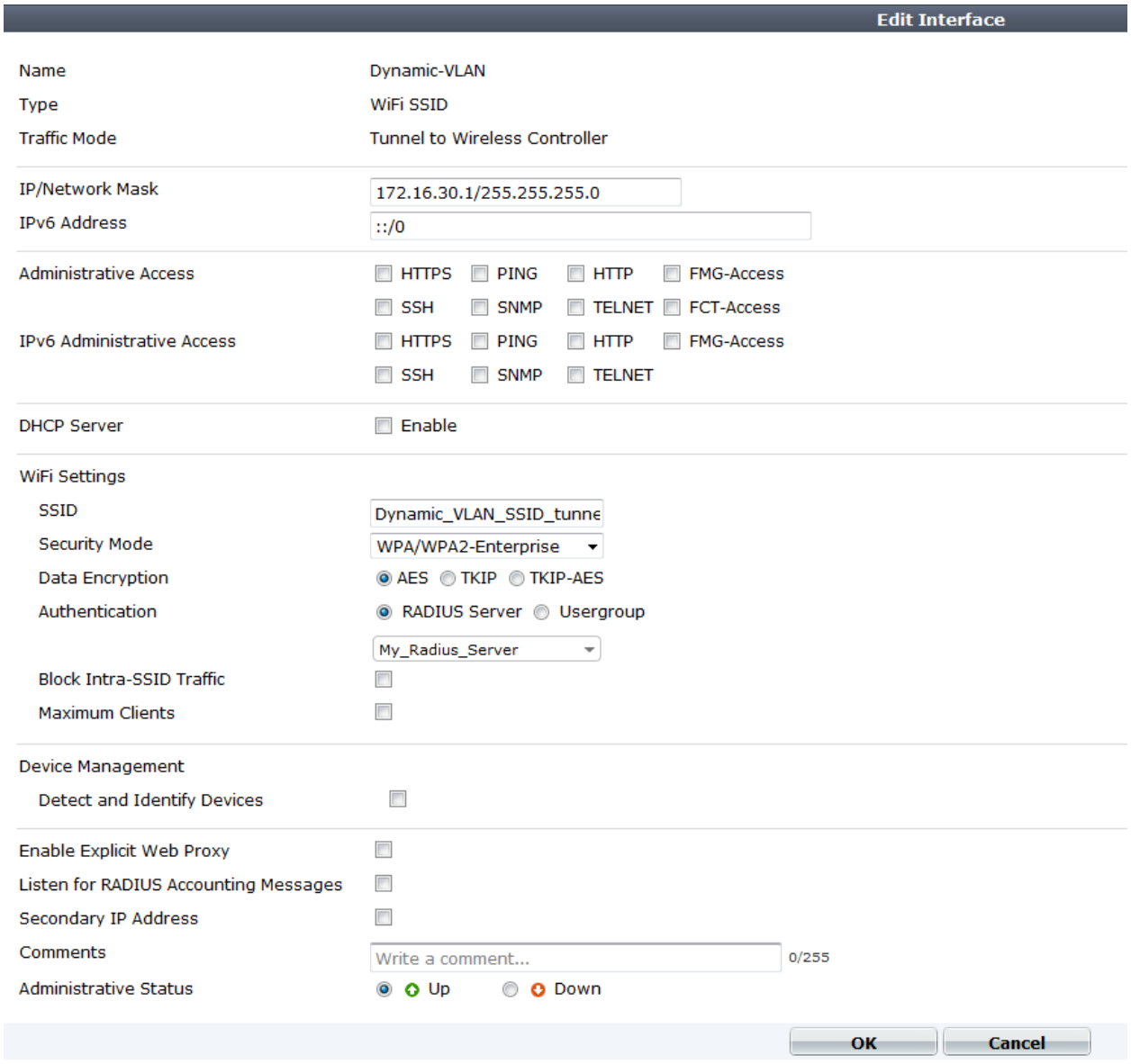
Connect the FortiAP to the FortiGate unit and go to Wifi Controller > Managed Access Points > Managed FortiAP and authorize the FortiAP



Go to User & Device > Authentication > RADIUS Server and create new



Go to WiFi Controller > WiFi Network > SSID and create new

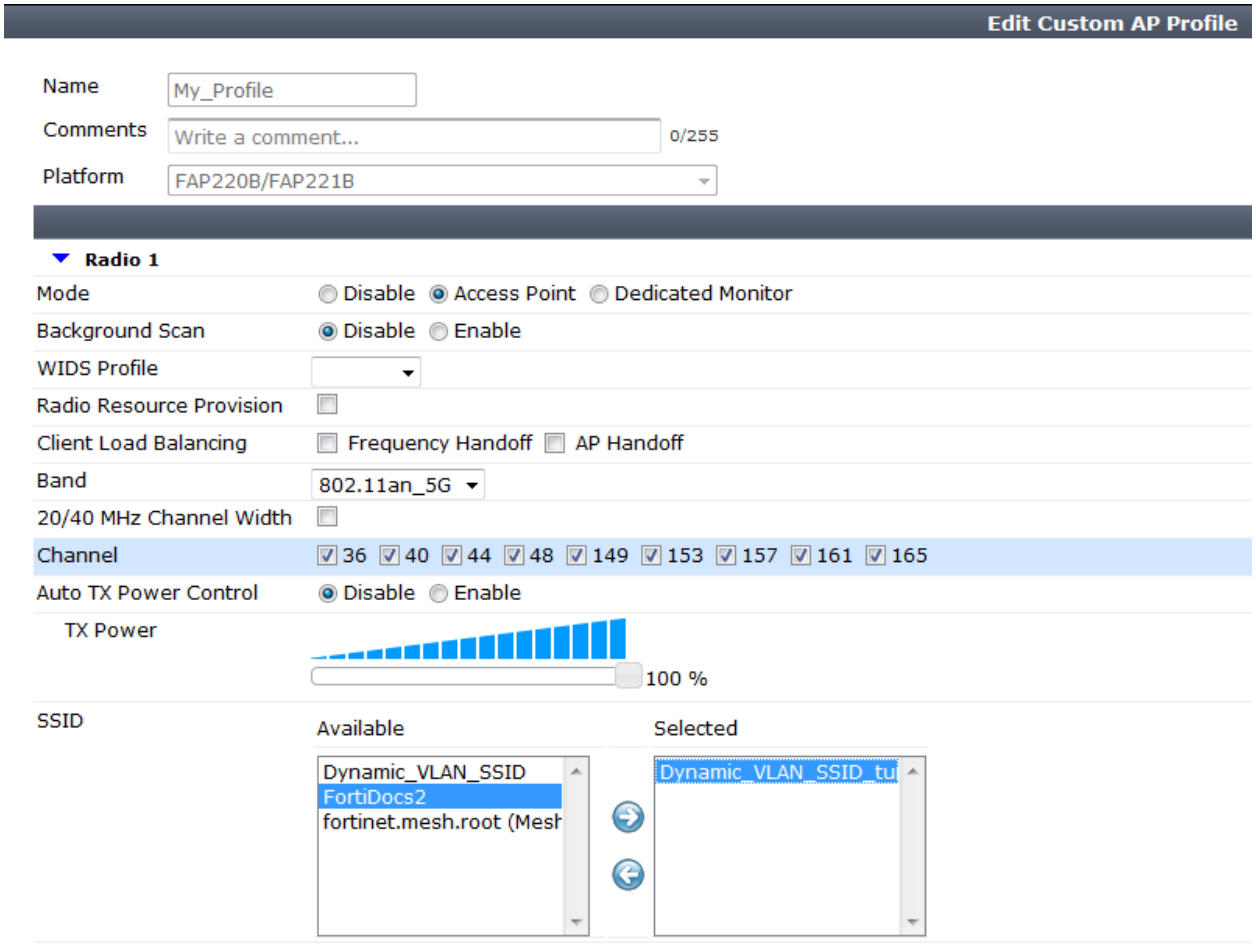


From CLI, you need to enable dynamic-vlan and optionally set a default vlanid

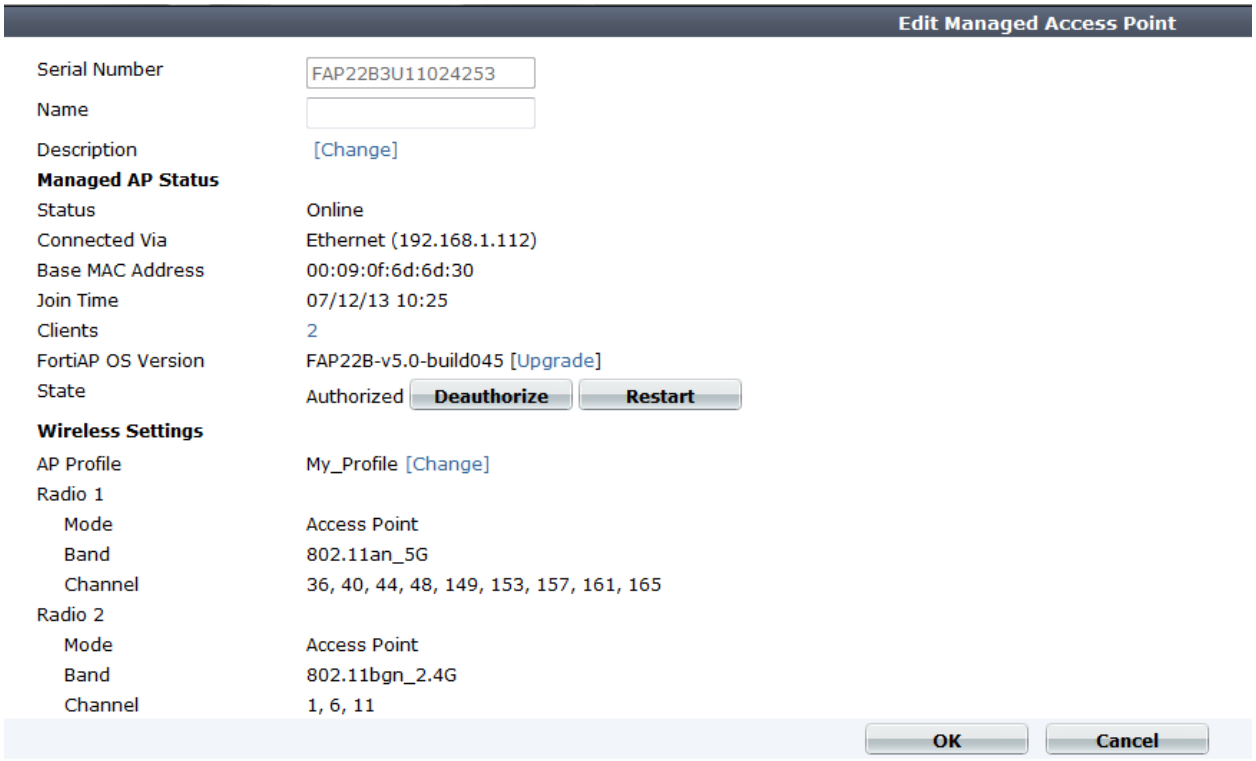
```
FG100D3G12801361 # config wireless-controller vap

FG100D3G12801361 (vap) # edit Dynamic-VLAN

FG100D3G12801361 (Dynamic-VLAN) # set vlanid 1

FG100D3G12801361 (Dynamic-VLAN) # set dynamic-vlan enable

FG100D3G12801361 (Dynamic-VLAN) # end

FG100D3G12801361 #
```

If dynamic-vlan is not enabled, all clients' traffic will use SSID's default vlan id which is 1.

Go to WiFi Controller > WiFi Network > Custom AP profile and create new and select “Dynamic_VLAN_SSID_tunnel_mode” under radio 1 and radio 2



Go to Wifi Controller > Managed Access Points > Managed FortiAP and edit the FortiAP and assign “My_Profile” under Wireless Settings > AP Profile



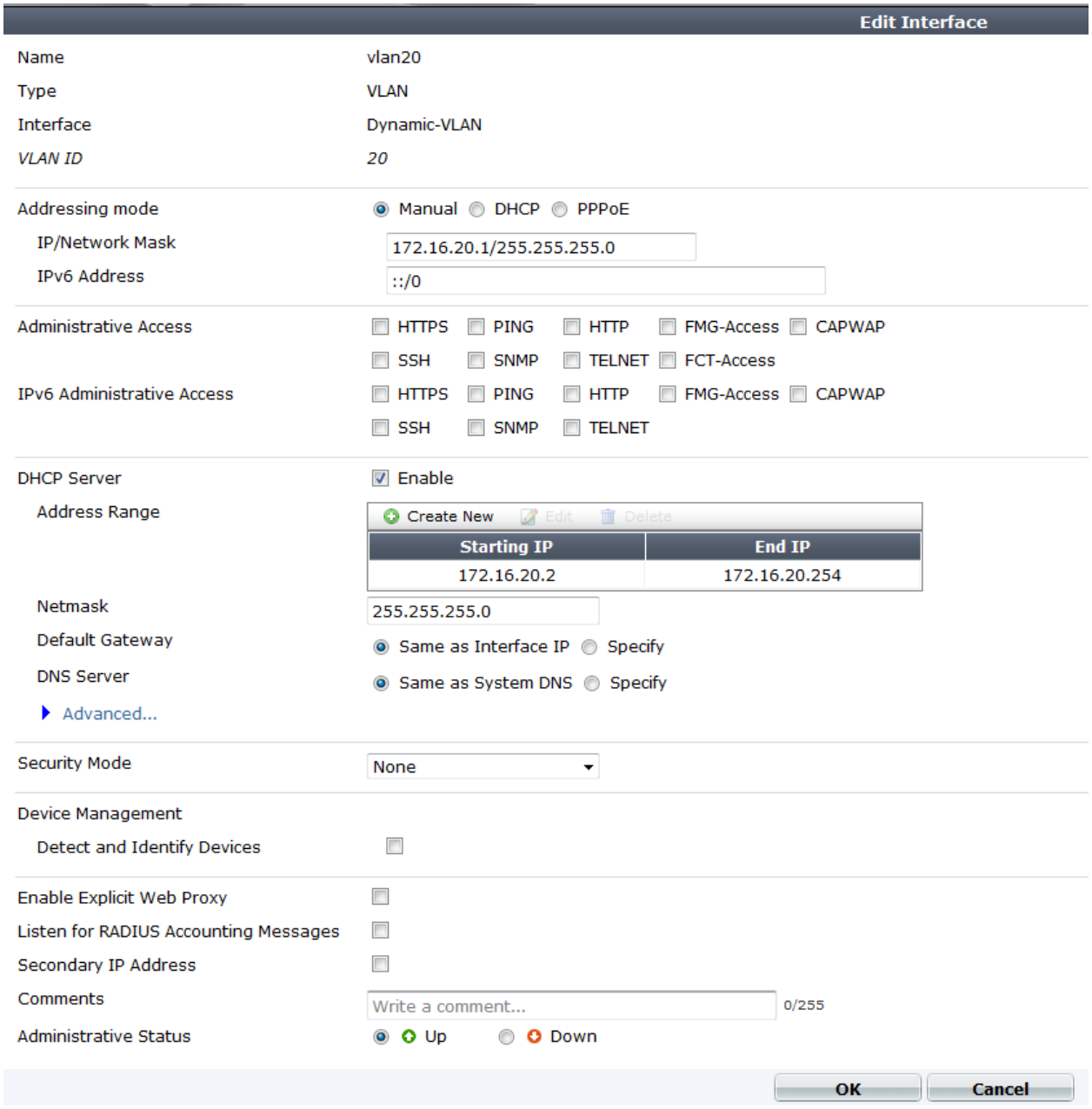
From CLI, create vlan-10 and vlan-20 under “Dynamic-VLAN” interface

```
FG100D3G12801361 (vlan10) # show
config system interface
    edit "vlan10"
        set vdom "root"
        set ip 172.16.10.1 255.255.255.0
        set snmp-index 36
        set interface "Dynamic-VLAN"
        set vlanid 10
    next
end

FG100D3G12801361 (vlan10) #
```

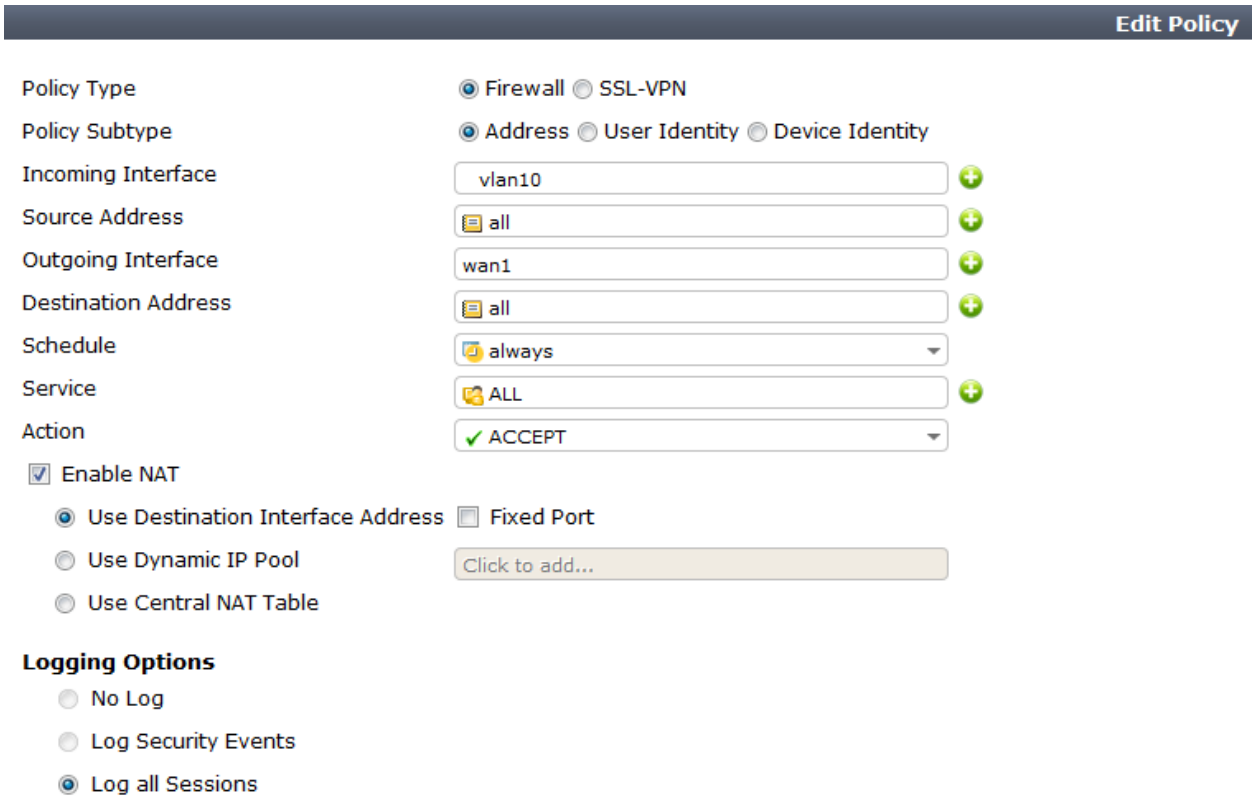
```
FG100D3G12801361 (vlan20) # show
config system interface
    edit "vlan20"
        set vdom "root"
        set ip 172.16.20.1 255.255.255.0
        set snmp-index 39
        set interface "Dynamic-VLAN"
        set vlanid 20
    next
end

FG100D3G12801361 (vlan20) #
```

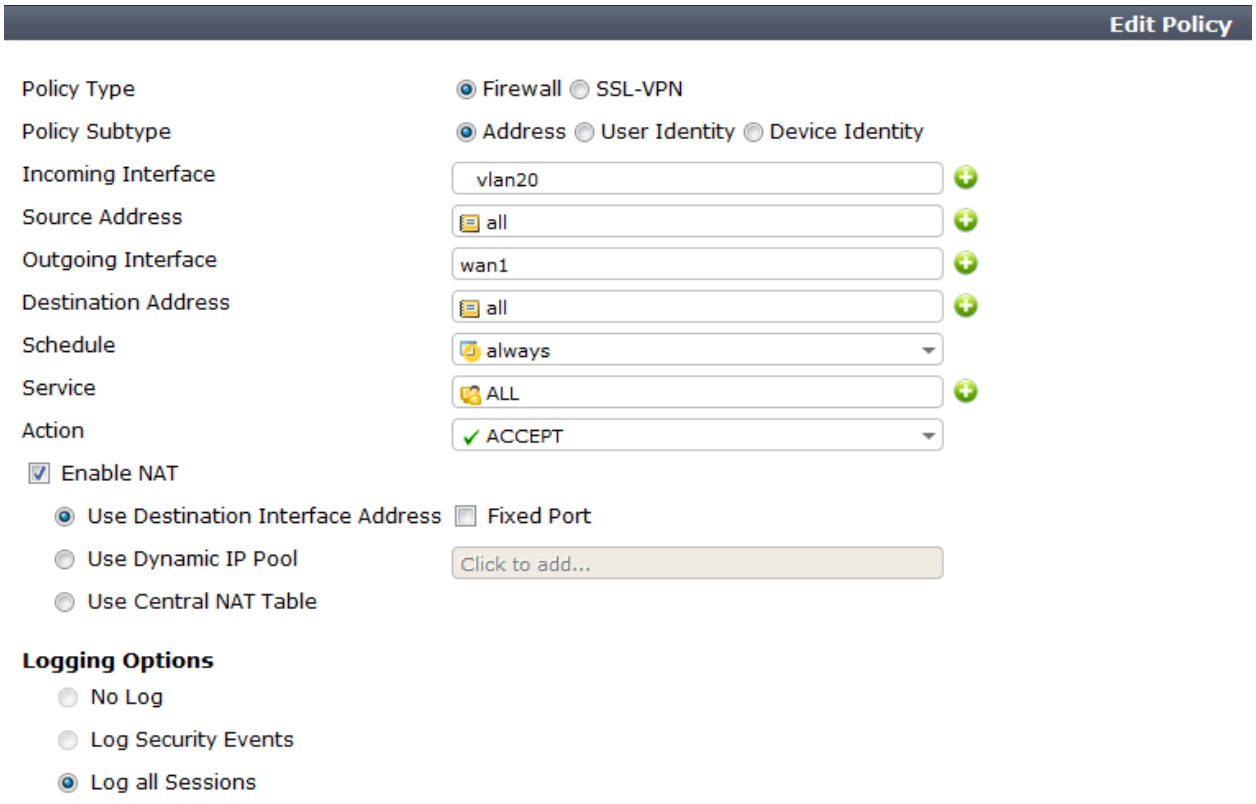
Then go to System > Network > Interface and enable DHCP server on vlan-10 and vlan-20


Edit Interface
Name
vlan10
Type
VLAN
Interface
Dynamic-VLAN
VLAN ID
10
Addressing mode
Manual
DHCP
PPPoE
IP/Network Mask
172.16.10.1/255.255.255.0
IPv6 Address
::/0
Administrative Access
HTTPS
PING
HTTP
FMG-Access
CAPWAP
SSH
SNMP
TELNET
FCT-Access
IPv6 Administrative Access
HTTPS
PING
HTTP
FMG-Access
CAPWAP
SSH
SNMP
TELNET
DHCP Server
Enable
Address Range
Create New
Edit
Delete
Starting IP
End IP
172.16.10.2
172.16.10.254
Netmask
255.255.255.0
Default Gateway
Same as Interface IP
Specify
DNS Server
Same as System DNS
Specify
Advanced...
Security Mode
None
Device Management
Detect and Identify Devices
Enable Explicit Web Proxy
Listen for RADIUS Accounting Messages
Secondary IP Address
Comments
Write a comment...
0/255
Administrative Status
Up
Down
OK
Cancel



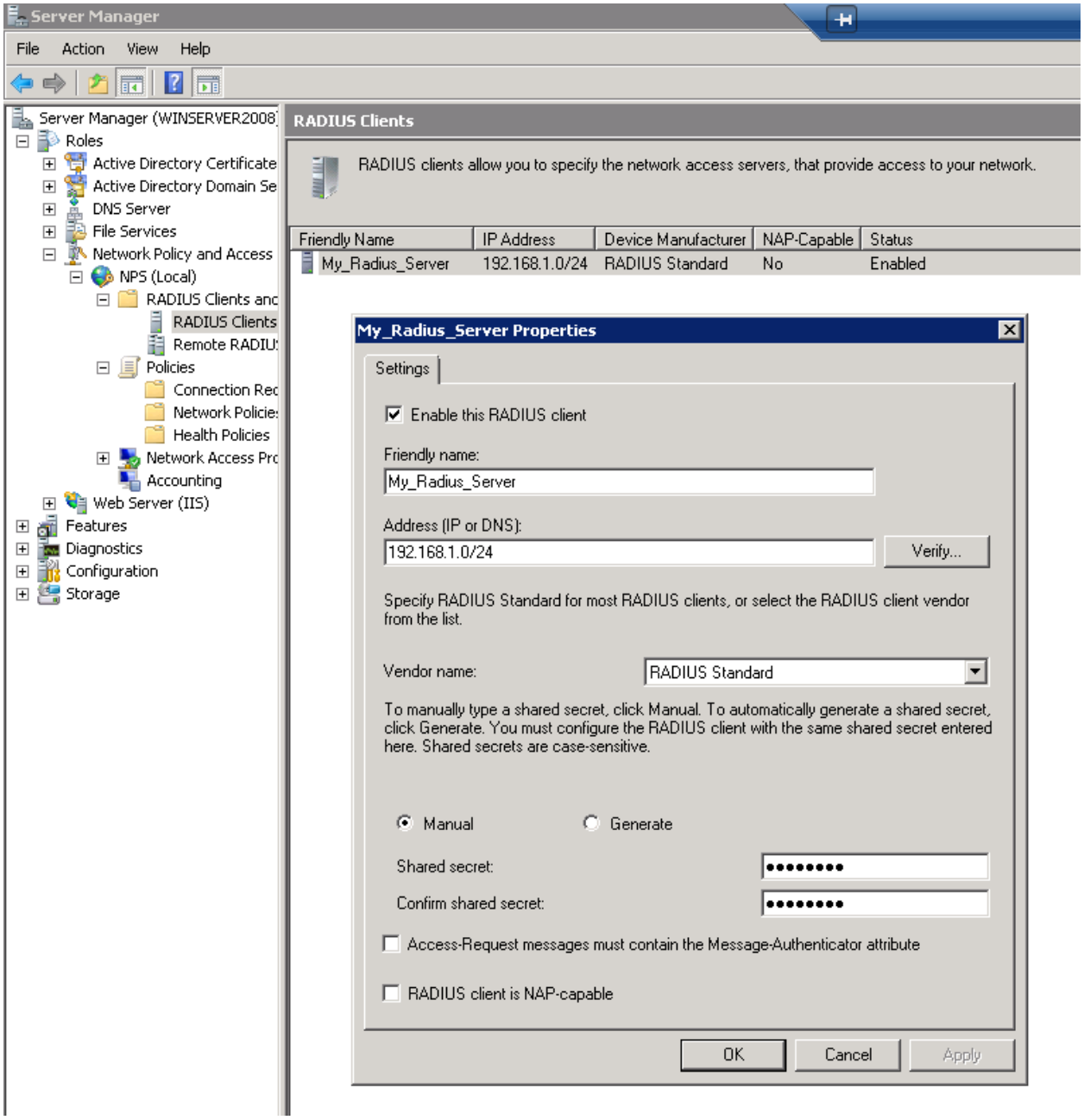
Go to Policy > Policy > Policy and create two security policies allowing outbound traffic from vlan-10 and vlan-20 respectively


Edit Policy
Policy Type
Firewall
SSL-VPN
Policy Subtype
Address
User Identity
Device Identity
Incoming Interface
vlan10
Source Address
all
Outgoing Interface
wan1
Destination Address
all
Schedule
always
Service
ALL
Action
ACCEPT
Enable NAT
Use Destination Interface Address
Fixed Port
Use Dynamic IP Pool
Click to add...
Use Central NAT Table
Logging Options
No Log
Log Security Events
Log all Sessions



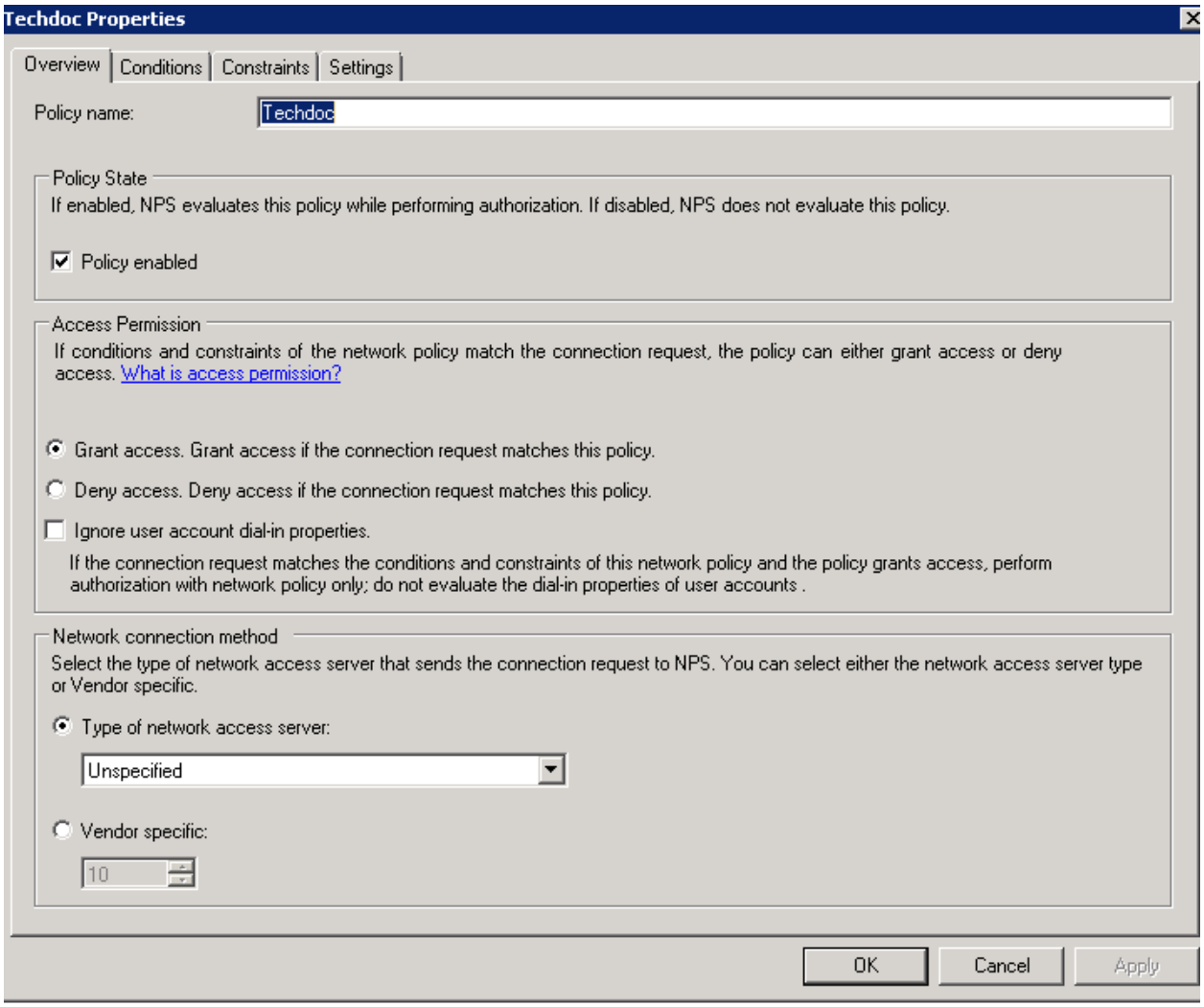
4. Configuring Radius server

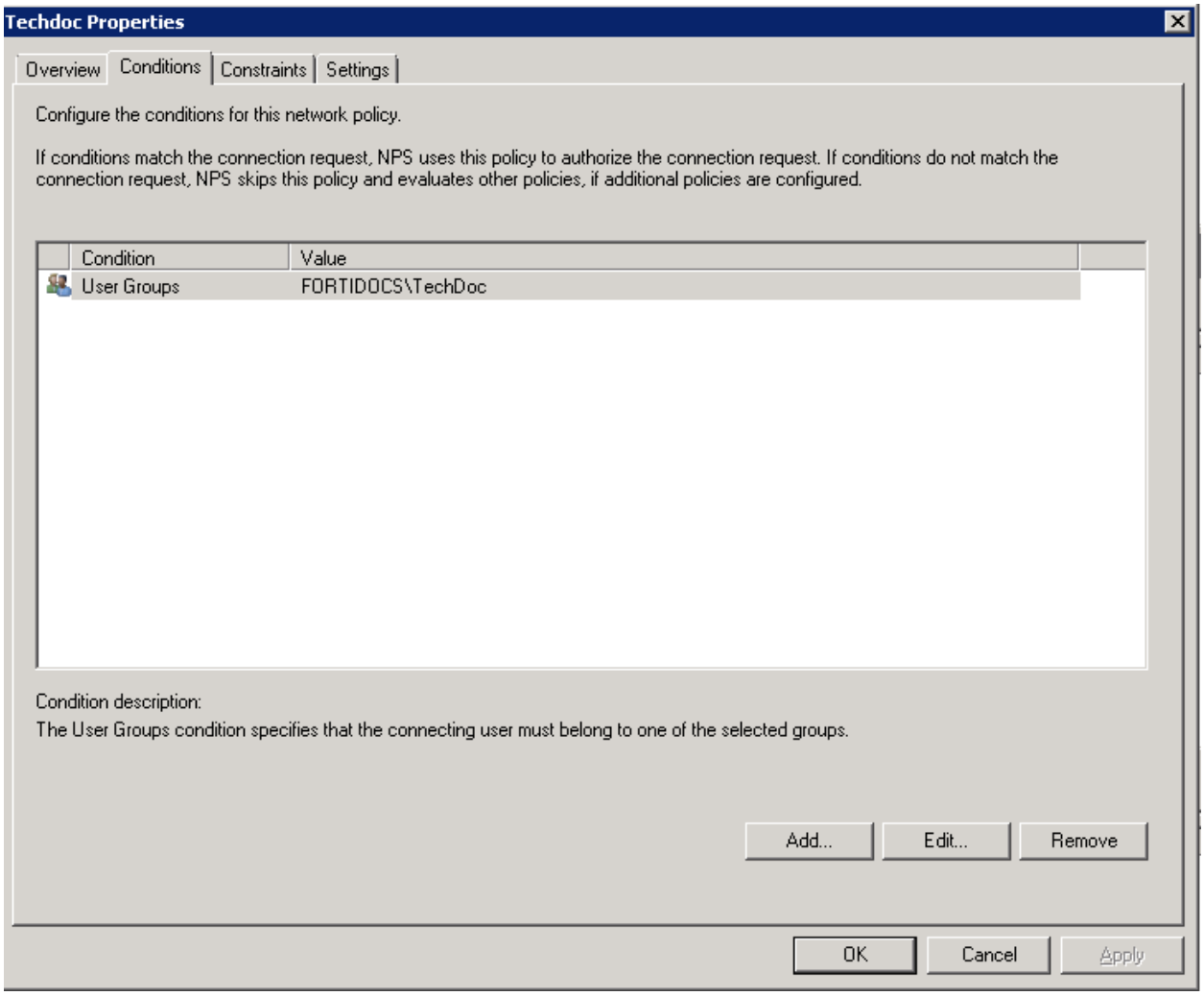
NPS on windows server 2008 is used for this example. Open Server Manager and create new RADIUS Client

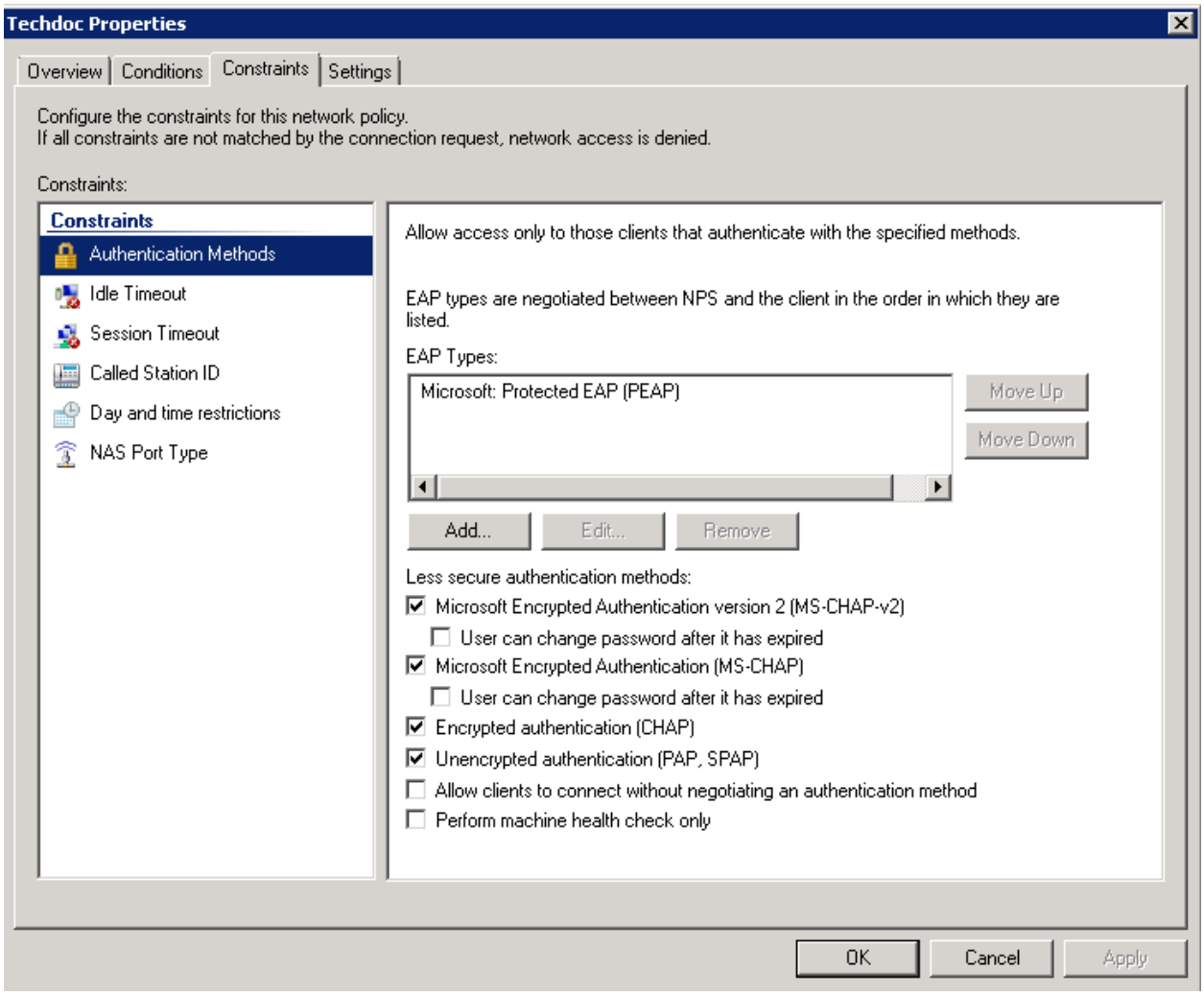


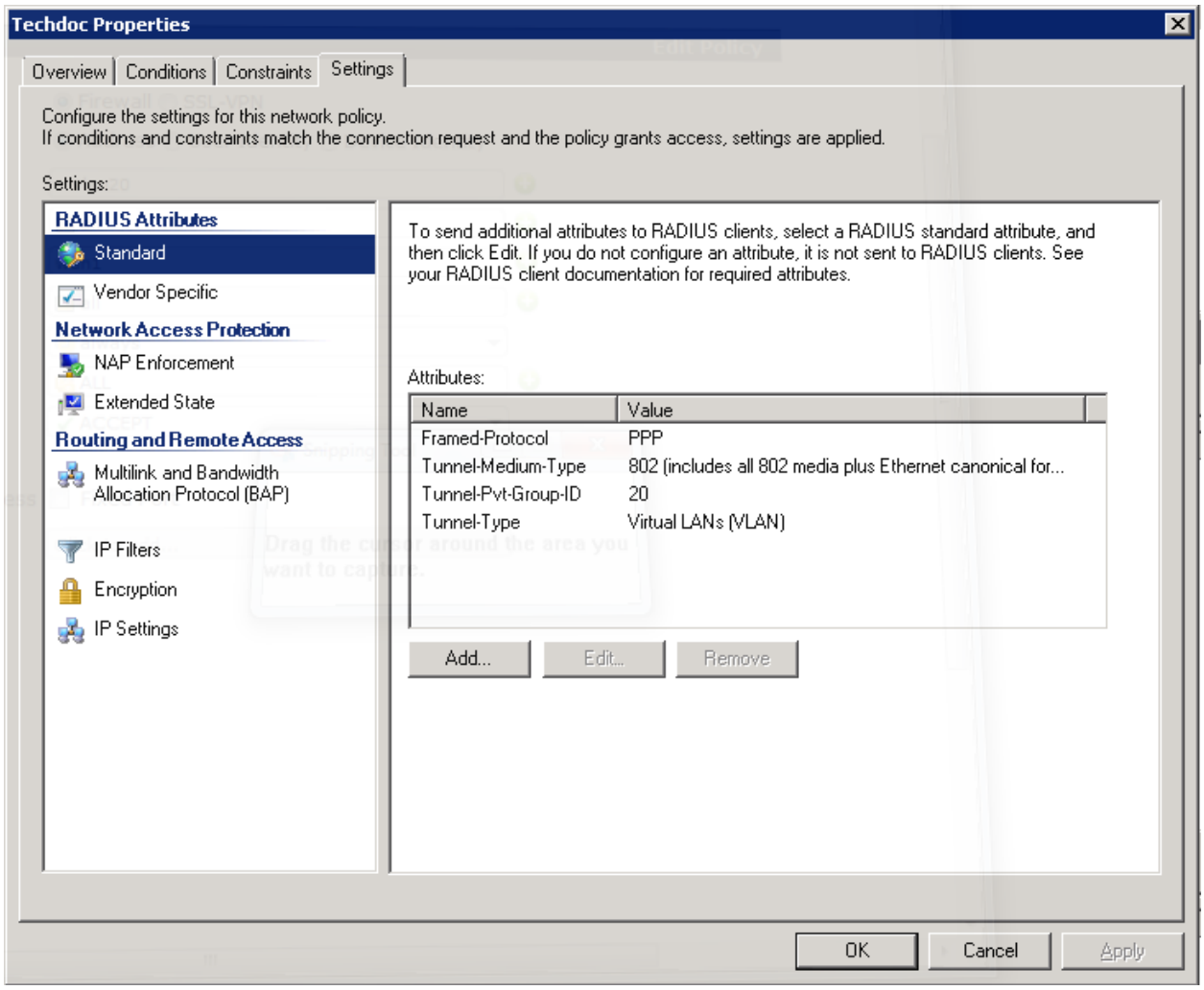
Then create two network policies, one for TechDoc user group and the other for Marketing user group.

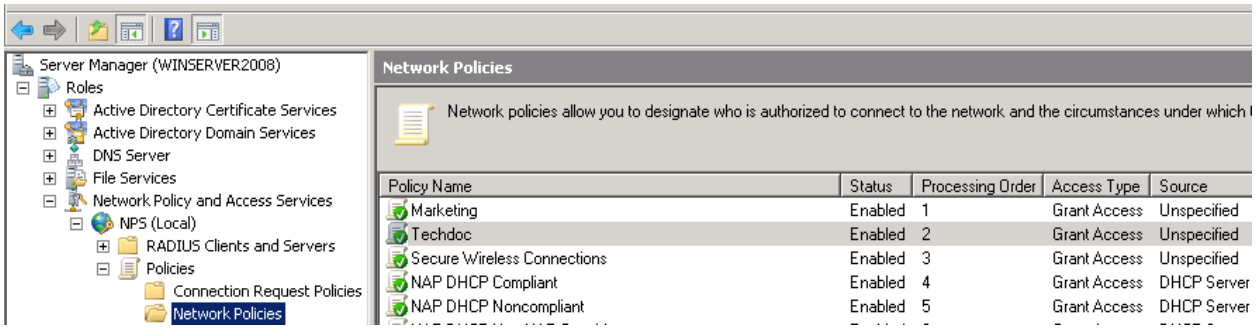
Set TechDoc user group to use Vlan 20 and Marketing user group to use Vlan 10


Techdoc Properties
Overview
Conditions
Constraints
Settings
Policy name:
Techdoc
Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.
Policy enabled
Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?
Grant access. Grant access if the connection request matches this policy.
Deny access. Deny access if the connection request matches this policy.
Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.
Type of network access server:
Unspecified
Vendor specific:
10
OK
Cancel
Apply


Techdoc Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
User Groups
FORTIDOCS\TechDoc
Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Add...
Edit...
Remove
OK
Cancel
Apply

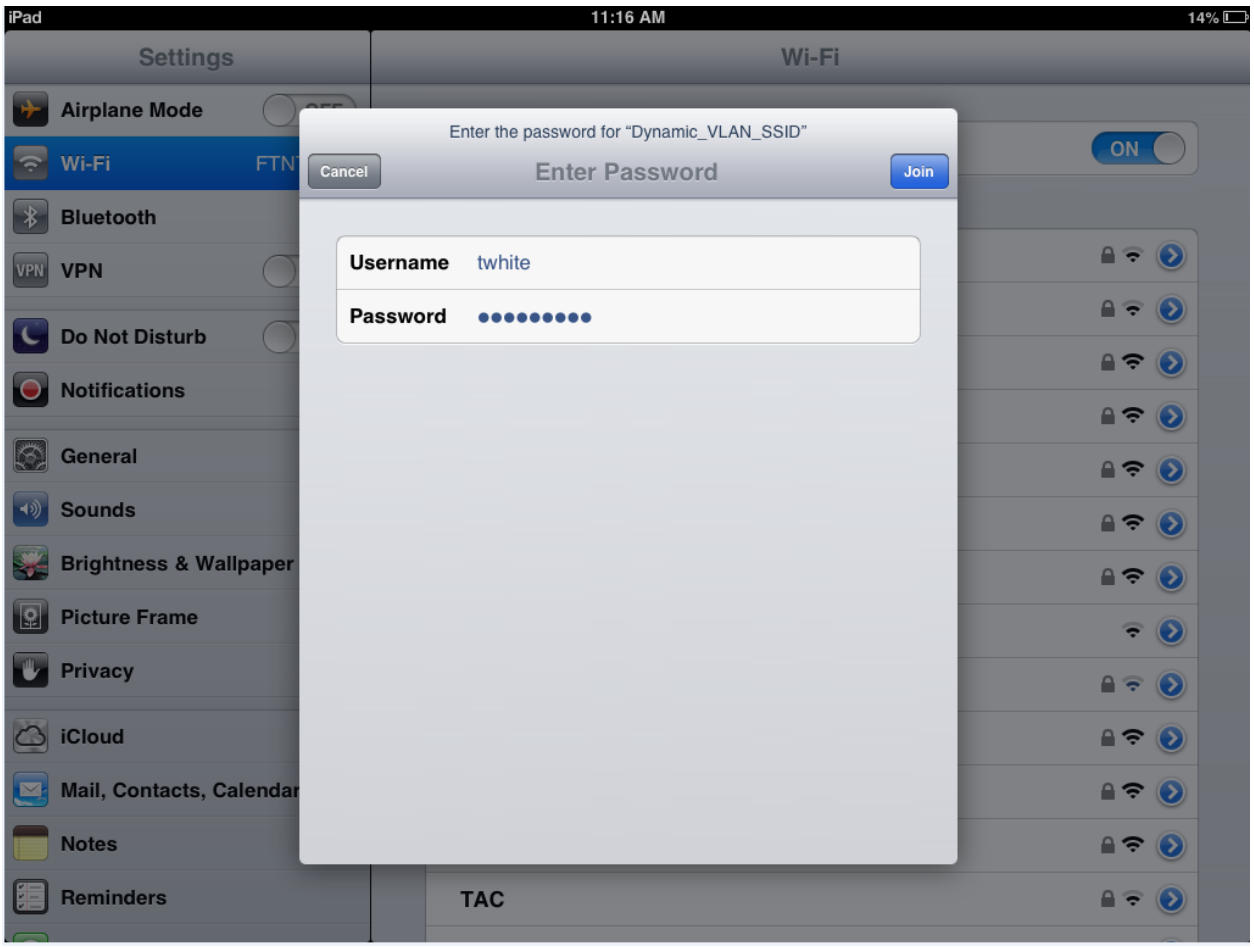

Techdoc Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Protected EAP (PEAP)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
Perform machine health check only
OK
Cancel
Apply

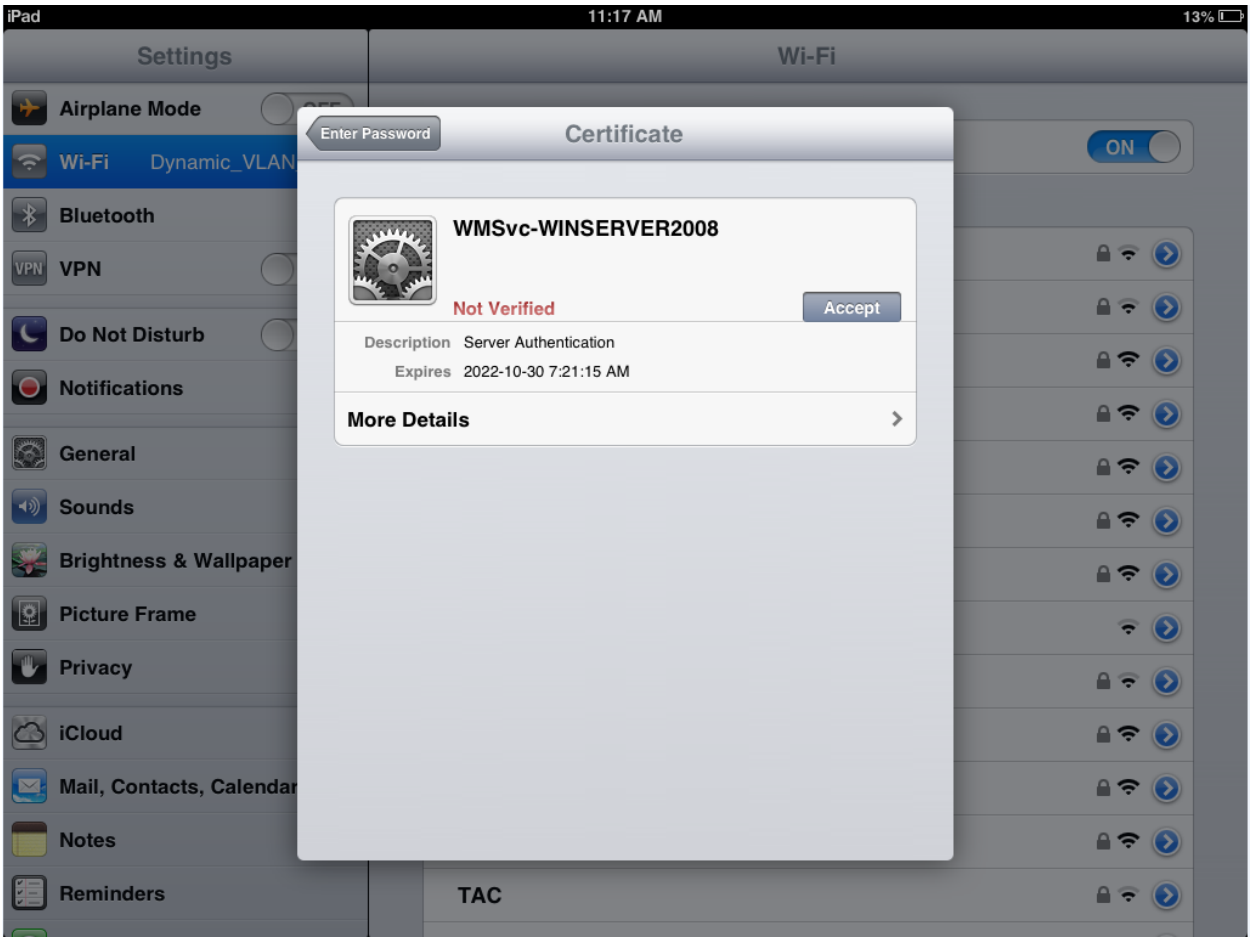

Techdoc Properties
Overview
Conditions
Constraints
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Framed-Protocol
PPP
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
20
Tunnel-Type
Virtual LANs (VLAN)
Add...
Edit...
Remove
OK
Cancel
Apply


Server Manager (WINSERVER2008)
Roles
Active Directory Certificate Services
Active Directory Domain Services
DNS Server
File Services
Network Policy and Access Services
NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Policies
Network Policies
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which
Policy Name
Status
Processing Order
Access Type
Source
Marketing
Enabled
1
Grant Access
Unspecified
Techdoc
Enabled
2
Grant Access
Unspecified
Secure Wireless Connections
Enabled
3
Grant Access
Unspecified
NAP DHCP Compliant
Enabled
4
Grant Access
DHCP Server
NAP DHCP Noncompliant
Enabled
5
Grant Access
DHCP Server

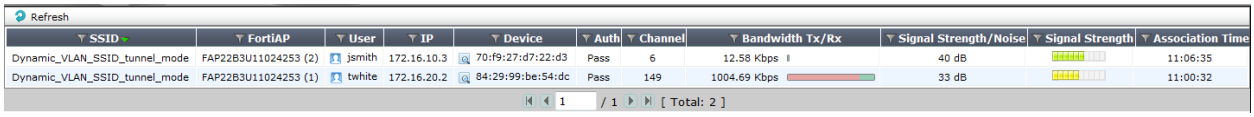
5. Result

Users scan for available SSID and connect to “Dynamic_VLAN_SSID_tunnel_mode” using their credentials





Based on the credential provided, a vlan 10 will be assigned to the Marketing user group and a vlan 20 to TechDoc user group

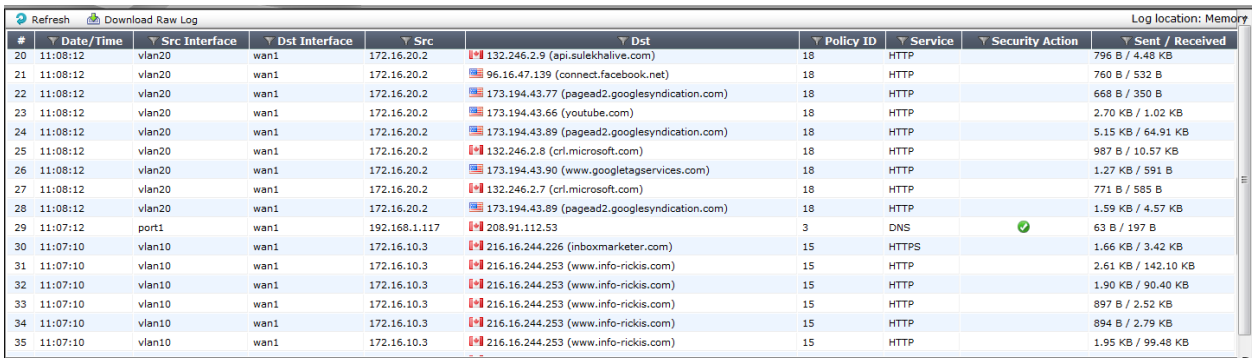


SSID	FortiAP	User	IP	Device	Auth	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal Strength	Association Time
Dynamic_VLAN_SSID_tunnel_mode	FAP22B3U11024253 (2)	jsmith	172.16.10.3	70:f9:27:d7:22:d3	Pass	6	12.58 Kbps	40 dB		11:06:35
Dynamic_VLAN_SSID_tunnel_mode	FAP22B3U11024253 (1)	twhite	172.16.20.2	84:29:99:be:54:dc	Pass	149	1004.69 Kbps	33 dB		11:00:32

Refresh

1 / 1 [Total: 2]

Go to Log & Report > Traffic Log > Forward Traffic



Refresh Download Raw Log Log location: Memory

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Policy ID	Service	Security Action	Sent / Received
20	11:08:12	vlan20	wan1	172.16.20.2	132.246.2.9 (api.sulekhalive.com)	18	HTTP		796 B / 4.48 KB
21	11:08:12	vlan20	wan1	172.16.20.2	96.16.47.139 (connect.facebook.net)	18	HTTP		760 B / 532 B
22	11:08:12	vlan20	wan1	172.16.20.2	173.194.43.77 (pagead2.googlesyndication.com)	18	HTTP		668 B / 350 B
23	11:08:12	vlan20	wan1	172.16.20.2	173.194.43.66 (youtube.com)	18	HTTP		2.70 KB / 1.02 KB
24	11:08:12	vlan20	wan1	172.16.20.2	173.194.43.89 (pagead2.googlesyndication.com)	18	HTTP		5.15 KB / 64.91 KB
25	11:08:12	vlan20	wan1	172.16.20.2	132.246.2.8 (crl.microsoft.com)	18	HTTP		987 B / 10.57 KB
26	11:08:12	vlan20	wan1	172.16.20.2	173.194.43.90 (www.googletagservices.com)	18	HTTP		1.27 KB / 591 B
27	11:08:12	vlan20	wan1	172.16.20.2	132.246.2.7 (crl.microsoft.com)	18	HTTP		771 B / 585 B
28	11:08:12	vlan20	wan1	172.16.20.2	173.194.43.89 (pagead2.googlesyndication.com)	18	HTTP		1.59 KB / 4.57 KB
29	11:07:12	port1	wan1	192.168.1.117	208.91.112.53	3	DNS	✓	63 B / 197 B
30	11:07:10	vlan10	wan1	172.16.10.3	216.16.244.226 (inboxmarketer.com)	15	HTTPS		1.66 KB / 3.42 KB
31	11:07:10	vlan10	wan1	172.16.10.3	216.16.244.253 (www.info-rickis.com)	15	HTTP		2.61 KB / 142.10 KB
32	11:07:10	vlan10	wan1	172.16.10.3	216.16.244.253 (www.info-rickis.com)	15	HTTP		1.90 KB / 90.40 KB
33	11:07:10	vlan10	wan1	172.16.10.3	216.16.244.253 (www.info-rickis.com)	15	HTTP		897 B / 2.52 KB
34	11:07:10	vlan10	wan1	172.16.10.3	216.16.244.253 (www.info-rickis.com)	15	HTTP		894 B / 2.79 KB
35	11:07:10	vlan10	wan1	172.16.10.3	216.16.244.253 (www.info-rickis.com)	15	HTTP		1.95 KB / 99.48 KB

Select an entry for details

Dst	132.246.2.9 (api.sulekhalive.com)	**Virtual Domain**	root
Received	4585	**Source Country**	Reserved
Src NAT IP	172.20.120.123	**Sent / Received**	796 B / 4.48 KB
Duration	57	**Sent**	796
Src NAT Port	50258	**Application Details**	
Service	HTTP	**Protocol**	6
Destination Country	Canada	**Dst Port**	80
Status	close	**Timestamp**	Thu Jul 25 11:08:12 2013
Tran Display	snat	**Sequence Number**	97889
Policy ID	18	**Src Interface**	vlan20
Src	172.16.20.2	**Sent Packets**	7
Level	notice	**Src Port**	50258
Log ID	13	**Sub Type**	forward
Threat		**Received Packets**	6
Date/Time	11:08:12 (Thu Jul 25 11:08:12 2013)	**Dst Interface**	wan1

Dst	216.16.244.226 (inboxmarketer.com)	**Virtual Domain**	root
Received	3500	**Source Country**	Reserved
Src NAT IP	172.20.120.123	**Sent / Received**	1.66 KB / 3.42 KB
Duration	9	**Sent**	1696
Src NAT Port	53679	**Application Details**	
Service	HTTPS	**Protocol**	6
Destination Country	Canada	**Dst Port**	443
Status	close	**Timestamp**	Thu Jul 25 11:07:10 2013
Tran Display	snat	**Sequence Number**	97779
Policy ID	15	**Src Interface**	vlan10
Src	172.16.10.3	**Sent Packets**	12
Level	notice	**Src Port**	53679
Log ID	13	**Sub Type**	forward
Threat		**Received Packets**	7
Date/Time	11:07:10 (Thu Jul 25 11:07:10 2013)	**Dst Interface**	wan1